PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-276444
(43)Date of publication of application : 06.10.2000

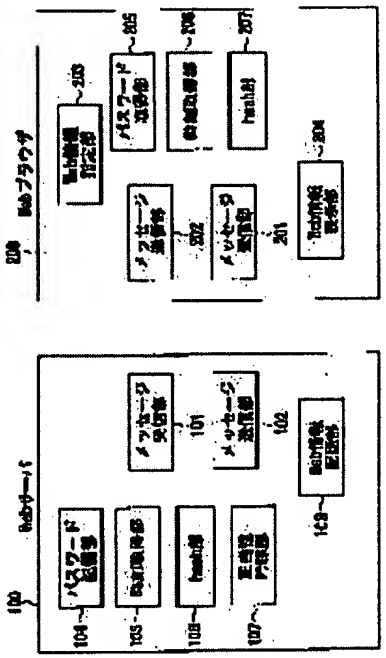
(51)Int.Cl. G06F 15/00
H04L 9/32

(21)Application number : 11-076875
(22)Date of filing : 19.03.1999

(71)Applicant : CANON INC
(72)Inventor : KUROSAWA TAKAHIRO

(54) COMMUNICATION EQUIPMENT, COMMUNICATION SYSTEM, AND COMPUTER READABLE STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To securely perform authentication by only performing unidirectional communication on a network once.
SOLUTION: In a Web browser 200, a first time from a time acquisition part 206 and a password from a password part 205 are operated in a hash part 207, and a message including this first operation result and the first time is transmitted from a message transmission part 202 to a Web server 100. In the Web server 100, the received first time and a password in a password storage part 104 are operated in a hash part 106 to obtain a second operation result. A validity examination part 107 compares a second time from a time acquisition part 105 with the first time, and it is decided that the receiver message is valid when the second time is later than the first time and the first operation result is matched with the second operation result.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－276444
（P2000－276444A）
(43)公開日　平成12年10月６日(2000.10.6)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４
			６７３Ｄ	

審査請求　未請求　請求項の数14　ＯＬ　（全９頁）

(21)出願番号　特願平11－76875

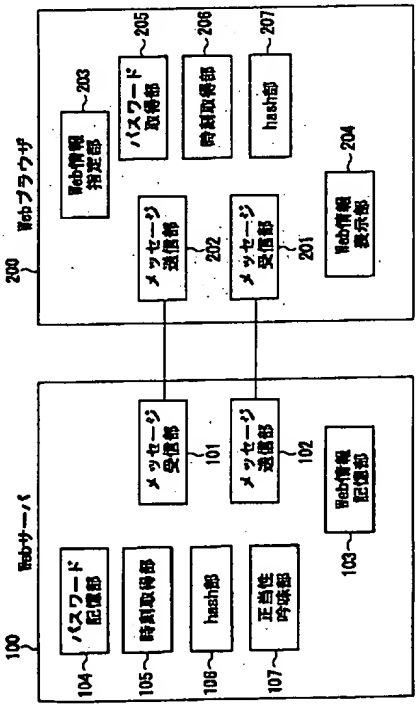
(22)出願日　平成11年３月19日(1999.3.19)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　黒澤　貴弘
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

Ｆターム(参考)　5B085 AC12 AE03 AE23
5J104 AA07 KA01 KA03 KA04 NA05
NA11 NA12 PA09

(54)【発明の名称】　通信装置、通信システム及びコンピュータ読み取り可能な記憶媒体

(57)【要約】
【課題】　ネットワーク上で単方向通信を１回行うだけで安全に認証を行うことができるようにする。
【解決手段】　Ｗｅｂブラウザ２００において、時刻取得部２０６からの第1の時刻とパスワード部２０５からのパスワードとをｈａｓｈ部２０７で演算し、その第1の演算結果と上記第1の時刻とを含むメッセージをメッセージ送信部２０２からＷｅｂサーバ１００に送信する。Ｗｅｂサーバ１００では、受信した第1の時刻とパスワード記憶部１０４のパスワードとをｈａｓｈ部１０６で演算して第2の演算結果を得る。そして、正当性吟味部１０７において、時刻取得部１０５からの第2の時刻と上記第1の時刻とを比較し、第2の時刻が第1の時刻より後で、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記受信したメッセージが正当であると判定する。



1

【特許請求の範囲】

【請求項1】 時刻を取得する時刻取得手段と、
パスワードを入力するパスワード入力手段と、
上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算手段と、
上記演算結果と上記時刻とを含むメッセージを作成して送信する送信手段とを設けたことを特徴とする通信装置。

【請求項2】 第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信手段と、
上記受信時の第2の時刻を取得する時刻取得手段と、
上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算手段と、
上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを設けたことを特徴とする通信装置。

【請求項3】 上記判定手段は、上記第1の時刻と第2の時刻との差の時間が所定時間以内であり、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記メッセージが正当であると判定することを特徴とする請求項2記載の通信装置。

【請求項4】 上記第1の時刻を記憶する記憶手段を設け、上記判定手段は、次回に受信したメッセージに含まれる第1の時刻が上記記憶した第1の時刻より未来であるか否かを判定することを特徴とする請求項2記載の通信装置。

【請求項5】 上記メッセージは送信元情報を含み、複数の第1の通信装置にそれぞれ対応して上記所定時間を登録した登録手段を設け、上記判定手段は、上記送信元情報と対応する上記登録された所定時間と上記差の時間とを比較することを特徴とする請求項2記載の通信装置。

【請求項6】 時刻を取得する第1の時刻取得手段と、パスワードを入力するパスワード入力手段と、上記取得した第1の時刻と入力されたパスワードとを不可逆に加工演算して第1の演算結果を出力する第1の演算手段と、上記第1の演算結果と上記第1の時刻とを含むメッセージを作成して送信する送信手段とを有する第1の通信装置と、
上記メッセージを受信する受信手段と、上記受信時の第2の時刻を取得する第2の時刻取得手段と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する第2の演算手段と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記第1の演算結果と第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを有する第2の通信装置とからなる通信システム。

2

【請求項7】 上記判定手段は、上記第1の時刻と第2の時刻との差の時間が所定時間以内であり、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記メッセージが正当であると判定することを特徴とする請求項6記載の通信システム。

【請求項8】 上記第2の通信装置に上記第1の時刻を記憶する記憶手段を設け、上記判定手段は、上記受信したメッセージに含まれる第1の時刻が上記記憶した第1の時刻より未来であるか否かを判定することを特徴とする請求項6記載の通信システム。

【請求項9】 複数の上記第1の通信装置が設けられ、各第1の通信装置は送信元情報を含む上記メッセージを送信し、上記第2の通信装置に上記複数の第1の通信装置にそれぞれ対応して上記所定時間を登録した登録手段を設け、上記判定手段は、上記送信元情報と対応する上記登録された所定時間と上記差の時間とを比較することを特徴とする請求項6記載の通信システム。

【請求項10】 時刻を取得する時刻取得処理と、
パスワードを入力するパスワード入力処理と、
上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算処理と、
上記演算結果と上記時刻とを含むメッセージを作成して送信する送信処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項11】 第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信処理と、
上記受信時の第2の時刻を取得する時刻取得処理と、
上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算処理と、
上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項12】 上記判定処理は、上記第1の時刻と第2の時刻との差の時間が所定時間以内であり、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記メッセージが正当であると判定することを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項13】 受信したメッセージに含まれる時刻を記憶する記憶処理を上記プログラムに設け、上記判定処理は、受信したメッセージに含まれる時刻が上記記憶した時刻より未来であるか否かを判定することを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項14】 上記メッセージは送信元情報を含み、上記判定処理は、複数の送信元にそれぞれ対応して予め登録された上記所定時間のうちの上記送信元情報と対応する所定時間と上記差の時間とを比較することを特徴と

3

する請求項11記載のコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク上のサーバが遠隔地にあるクライアントの正当性を認証するようにした通信システムに用いて好適な、上記サーバ及びクライアントが用いる通信装置、この通信装置を有する通信システム及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【0002】

【従来の技術】近年、以下に列挙するような認証に関する技術あるいは製品が提供されるようになってきた。

・一方向関数を用いた認証方法

入力を不可逆に加工する関数を用いる。これは、その関数の出力結果から関数の入力(引数)となった情報を推測することが難しい関数である。例えばRFC1321に示されるMD5などの関数であり、Massage Digestの作成などにも利用される。実装上はハッシュ(hash)関数として知られる関数が利用されることもある。

【0003】・one－time パスワード型認証方法

インターネットなどのネットワークの発達にともなって、ネットワーク上を流れるパケットを覗き見するなどの手法によるアカウントやパスワードの不正取得あるいは不正利用が行なわれるようになってきた。AT&TによるOTPなどに代表されるone－time パスワード型認証方法は、このような不正行為に対して防衛する目的で用いられている。この方法では、ネットワーク上を流れるパスワード情報は毎回変わるよう設計されている。

【0004】・challenge response型認証方法

上記と同様の目的で、challenge response型認証方法が用いられている。これは、接続リクエストを発行したクライアントに対してサーバ側から提供されるchallengeデータを、クライアント側でパスワードのhashに組み入れることで、パスワード自体は変化しないにも関わらず、hash結果のresponseデータの値が何回変わるように設計されている。このため、パスワード情報の送付に利用したパケットがネットワークの途中で覗き見されることがあっても、同一のパスワード情報が有効になることは、確率的に非常に少なく、パスワードの安全性が高められる〔図1(b)参照〕。

【0005】・NTP(Network Time Protocol)

ネットワーク接続されたコンピュータの内部時計を正しく調整するためのプロトコルとして、TP(Network Time Protocol;RFC1119)

4

が使われている。

【0006】

【発明が解決しようとする課題】しかしながら、従来のchallenge response型認証方法では、クライアントからの接続要求を受けてから。サーバ側で生成したchallengeデータをクライアント側に送り返し、さらにクライアント側でそのchallengeデータからresponseデータを生成してサーバ側に送るという手続きを取るために、一回の接続要求の認証のために、最低3回の通信パケットの送受信を必要としている。このことは、インターネットなどのように通信コストの大きなネットワークで利用されるアプリケーションの場合には、その応答性を落とすという問題があった。

【0007】本発明は、上記の問題を解決するために成されたもので、一回の接続要求の認証のために、一回の通信パケットの送受信で済ませることができるようにすることを目的としている。

【0008】

【課題を解決するための手段】上記の目的を達成するために、本発明による通信装置においては、時刻を取得する時刻取得手段と、パスワードを入力するパスワード入力手段と、上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算手段と、上記演算結果と上記時刻とを含むメッセージを作成して送信する送信手段とを設けている。

【0009】また、本発明による他の通信装置においては、第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信手段と、上記受信時の第2の時刻を取得する時刻取得手段と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算手段と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを設けている。

【0010】また、本発明による通信システムにおいては、時刻を取得する第1の時刻取得手段と、パスワードを入力するパスワード入力手段と、上記取得した第1の時刻と入力されたパスワードとを不可逆に加工演算して第1の演算結果を出力する第1の演算手段と、上記第1の演算結果と上記第1の時刻とを含むメッセージを作成して送信する送信手段とを有する第1の通信装置と、上記メッセージを受信する受信手段と、上記受信時の第2の時刻を取得する第2の時刻取得手段と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する第2の演算手段と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記第1の演算結果と第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを有する第

5

２の通信装置とを設けている。

【００１１】また、本発明による記憶媒体においては、時刻を取得する時刻取得処理と、パスワードを入力するパスワード入力処理と、上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算処理と、上記演算結果と上記時刻とを含むメッセージを作成して送信する送信処理とを実行するためのプログラムを記憶している。

【００１２】また、本発明による他の記憶媒体においては、第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信処理と、上記受信時の第2の時刻を取得する時刻取得処理と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算処理と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定処理とを実行するためのプログラムを記憶している。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。

（第1の実施の形態）図2は、本発明をＷｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ（以下、Ｗｅｂと略す）サーバ及びクライアントとしてのＷｅｂブラウザに用いた場合の通信システムを示すブロック図である。図2において、１００は本実施の形態による認証機能を有するＷｅｂサーバ、２００は本実施の形態によるメッセージを送信するＷｅｂブラウザである。

【００１４】Ｗｅｂサーバ１００とＷｅｂブラウザ２００はそれぞれネットワーク３００に接続され、Ｗｅｂブラウザ２００からネットワーク３００を介してＷｅｂページ情報のリクエストがＷｅｂサーバ１００へメッセージとして送られる。Ｗｅｂサーバ１００では、まず、受信したメッセージの正当性を判断し、正当であることが認められると、Ｗｅｂブラウザ２００へ上記リクエストされたＷｅｂページ情報を送付する。Ｗｅｂブラウザ２００では、受信したＷｅｂページ情報を表示することができる。

【００１５】尚、この図2のネットワーク３００は、企業あるいは組織内で運用されるイントラネットである場合もあり、あるいは広く世界をつないでいるインターネットである場合もある。

【００１６】図3はＷｅｂサーバ１００を動作させるハードウエアの構成例を示すものであり、一般のコンピュータシステムで構成されている。即ち、プログラムを格納したＨＤ装置１０及びメモリ１１、ネットワーク３００と接続するためのネットワークＩ／Ｆ１２、プログラムによる各種の処理を実行するＣＰＵ１３、プログラムを媒体からロードするためのＦＤ装置１４、周辺コントローラ１５、表示ボード１６、マウス１７、キーボード１８、ディスプレイ装置１９などから構成されている。

6

【００１７】図4はＷｅｂブラウザ２００を動作させるハードウエアの構成例を示すものであり、一般のコンピュータシステムで構成されている。即ち、プログラムを格納したＨＤ装置２０及びメモリ２１、ネットワーク３００と接続するためのネットワークＩ／Ｆ２２、プログラムによる各種の処理を実行するＣＰＵ２３、プログラムを媒体からロードするためのＦＤ装置２４、周辺コントローラ２５、表示ボード２６、マウス２７、キーボード２８、ディスプレイ装置２９などから構成されている。

【００１８】図5はＷｅｂサーバ１００とＷｅｂブラウザ２００の構成を模式化したブロック図である。これらの各部の処理を実装したプログラムは、図3、図4のハードウェア構成上では、ＨＤ装置１０、２０やメモリ１１、２１あるいはＦＤ装置１４、２４に格納され、必要に応じてＣＰＵ１３、２３で実行される。

【００１９】Ｗｅｂサーバ１００は、ネットワーク３００上からデータを受け取るメッセージ受信部１０１と、ネットワーク上にデータを送り出すメッセージ送信部１０２と、個々のＷｅｂページ情報を記憶しておき、求めに応じてそれらを取り出すためのＷｅｂ情報記憶部１０３とからなる通常のＷｅｂサーバの構成に加えて、予めパスワードが登録されたパスワード記憶部１０４と、コンピュータ内の時刻情報を取得するための時刻取得部１０５と、不可逆な加工演算を行う一方向関数を提供するｈａｓｈ部１０６と、入力された時刻情報やｈａｓｈ結果から要求の正当性を判断するための正当性吟味部１０７とから構成される。

【００２０】また、Ｗｅｂブラウザ２００は、ネットワーク上からデータを受け取るメッセージ受信部２０１と、ネットワーク上にデータを送り出すメッセージ送信部２０２と、ユーザの求めるＷｅｂ情報を指定するＵＲＬなどを得るためのＷｅｂ情報指定部２０３と、受信したＷｅｂページ情報を表示するためのＷｅｂ情報表示部２０４とからなる通常のＷｅｂブラウザの構成に加えて、キーボードなどの入力装置からユーザ固有のパスワードを得るためのパスワード取得部２０５と、上記Ｗｅｂサーバ１００と同様の時刻取得部２０６と、上記Ｗｅｂサーバ１００と同一のｈａｓｈ部２０７とから構成される。

【００２１】図6はＷｅｂブラウザ２００が実装したプログラムの処理を示すフローチャートである。Ｗｅｂブラウザ２００は、Ｗｅｂサーバ１００にアクセスしようとする際、まずＳ１００１ステップ（以下、ステップ略）で、Ｗｅｂ情報取得部２０３からＵＲＬなどのＷｅｂ指定値報を得る。次にＳ１００２で、パスワード取得部２０５からパスワードを得る。続いてＳ１００３で、時刻取得部２０６から時刻を得る。そしてＳ１００４

7

で、それらのパスワードと時刻をｈａｓｈ部２０７によってｈａｓｈする。

【００２２】さらにＳ１００５で、そのｈａｓｈ結果に上記時刻、ユーザ名、Ｗｅｂ指定情報を添えてメッセージ送信部２０２からアクセス要求をＷｅｂサーバ１００に送る。その後、Ｓ１００６でＷｅｂサーバ１００からの返答を待つ。そして、Ｗｅｂサーバ１００でメッセージの正当性が認められるとＷｅｂサーバ１００からページ情報が送信されるので、Ｓ１００７で、メッセージ受信部２０１によりＷｅｂサーバ１００からのＷｅｂのページ情報を受け取る。続いてＳ１００８で、Ｗｅｂのページ情報をＷｅｂ情報表示部２０４で表示する。

【００２３】図7は、Ｗｅｂサーバ１００が実装したプログラムの処理を示すフローチャートである。最初にＳ２００１で、Ｗｅｂブラウザ１００からのアクセス要求を待つ。Ｓ２００２で、メッセージ受信部１０１からメッセージを得る。次にＳ２００３で、メッセージのユーザに相当するパスワードを、パスワード記憶部１０４から取り出す。続いてＳ２００４で、時刻取得部１０５からＷｅｂサーバ側の受信時刻Ｔ１を得る。

【００２４】そしてＳ２００５で、受信したメッセージからＷｅｂブラウザ側の時刻Ｔ２を取り出す。またＳ２００６で、パスワード記憶部１０４から得られたパスワードと上記時刻Ｔ２とを、Ｓ１００４と同様の手順でｈａｓｈ部１０６により計算し、そのｈａｓｈ結果Ｈ１を得る。また、メッセージからｈａｓｈ結果Ｈ２を取り出す。

【００２５】そしてＳ２００７で、上記時刻Ｔ１、Ｔ２及びｈａｓｈ結果Ｈ１、Ｈ２を正当性吟味部１０７で検討し、認証の可否を決定する。そしてＳ２００８で、認証が正当であるならば、メッセージ内のＷｅｂ指定情報から求められるＷｅｂページ情報をメッセージ送信部１０２によりＷｅｂブラウザ２００に送信する。また、認証が正当でないならばその旨返答する。最後にＳ２００１に戻り、次のアクセス要求を待ち合わせる。

【００２６】図8は、一方向関数を提供するｈａｓｈ部１０６及びｈａｓｈ部２０７の処理を実装したプログラムの処理を示すフローチャートである。ここでは、説明を簡単にするために、入力となるパスワードと時刻情報を文字列で表現し、かつ一方向関数として、ＲＦＣ１３２１に示されるＭＤ５関数を利用する場合について述べる。まずＳ３００１で、受け取ったパスワードと時刻情報を文字列化する。時刻情報に関しては、例えば、「１９９８／Ｊａｎ／０５．１３：３４：２０」のような形式で表現するものとする。

【００２７】次にＳ３００２で、文字列化したパスワードと時刻情報を結合してＭＤ５関数へ入力する。そしてＳ３００３で、ＭＤ５関数の出力をｈａｓｈ結果とする。例えば、パスワード「ｐａｓｐａｓｐａｓ」、時刻「１９９８／Ｊａｎ／０５．１３：３４：２０」と表される文字列を結合してＭＤ５に入力した場合、次のような出力が得られる。ＭＤ５（“ｐａｓｐａｓｐａｓ１９９８／Ｊａｎ／０５．１３：３４：２０”）＝“０ｅ４７ｅ１２１ｄ０４８０６５４３３ｂｂｆ８ｅｅｄ３４４６２５８”従って、上記「０ｅ４７ｅ１２１ｄ０４８０６５４３３ｂｂｆ８ｅｅｄ３４４６２５８」がｈａｓｈ結果となる。

8

【００２８】図9は、正当性吟味部１０７の処理を実装したプログラムの処理を示すフローチャートである。正当性吟味部１０７は、送られてきたメッセージに含まれる時刻Ｔ２とＷｅｂサーバ内の時刻Ｔ１、及び送られてきたメッセージに含まれるｈａｓｈ結果Ｈ２とＷｅｂサーバ内に記憶していたパスワードから生成したｈａｓｈ結果Ｈ１とを入力として与えられ、メッセージの正当性を判定するブール値を回答する。

【００２９】まずＳ４００１で、送られてきたメッセージ内の時刻Ｔ２とＷｅｂサーバ側の時刻Ｔ１とを比較し、Ｔ２がＴ１よりも過去であるならば、次のステップに進み、過去でないならば、ＦＡＬＳＥを回答する。次にＳ４００２で、送られてきたメッセージ内のｈａｓｈ結果Ｈ２とＷｅｂサーバ内に記憶していたパスワードから生成したｈａｓｈ結果Ｈ１とを比較し、一致したならば次のステップに進み、一致しないならば、ＦＡＬＳＥを回答する。次にＳ４００３で、ＴＲＵＥを回答する。

【００３０】本実施の形態では、パスワードと時刻とを入力としてｈａｓｈしているが、これに加えて、ユーザ名をｈａｓｈ部の入力に追加してもよい。また本実施の形態では、Ｗｅｂブラウザを独自プログラムとして説明したが、Ｎｅｔｓｃａｐｅ社のＮａｖｉｇａｔｏｒやＭｉｃｒｏｓｏｆｔ社のＩｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒなどのような汎用のＷｅｂブラウザ上で動作するＪＡＶＡプログラムやＡｃｔｉｖｅＸプログラムで実装することもできる。

【００３１】以上述べたように、ネットワーク上で利用されるプログラムの認証を行う場合に、パスワードのｈａｓｈ部に、時刻情報をも追加入力することにより、ｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ型認証よりも少ない通信コストでありながら同程度の安全性を提供することができる。

【００３２】（第2の実施の形態）第1の実施の形態では、正当性吟味部１０７は、前記Ｓ４００１において、送られてきたメッセージに含まれる時刻Ｔ２がＷｅｂサーバ内の時刻Ｔ１よりも過去である場合に正当と判定していたが、本実施の形態では、この部分に加えて、「同一ユーザの前回のアクセス要求のメッセージに含まれていた時刻Ｔ３よりも、今回のメッセージに含まれる時刻Ｔ２がより未来である場合のみ正当」と判定する点に特徴がある。

【００３３】このためには、前記Ｓ４００１の処理とＳ４００２の処理との間に、以下のようなステップＳ４２

０１を挿入するすることで実現できる。Ｓ４２０１では、送られてきたメッセージ内の時刻Ｔ２と、Ｗｅｂサーバ内に記憶されているユーザ情報内の前回アクセスの時刻Ｔ３とを比較し、今回のメッセージに含まれる時刻Ｔ２の方が未来であるならば、その時刻Ｔ２をユーザ情報内の前回のアクセス時刻として登録し、次のステップに進む。反対に、今回のメッセージに含まれる時刻の方が過去であるならば、ＦＡＬＳＥを回答する。これにより、Ｗｅｂブラウザからのメッセージの正当性をより厳密にチェックすることができる。

【００３４】（第3の実施の形態）第1の実施の形態では、正当性吟味部１０７は、Ｓ４００１において、送られてきたメッセージに含まれる時刻Ｔ２がＷｅｂサーバ内の時刻Ｔ１よりも過去である場合に正当と判定していたが、本実施の形態では、この部分を「Ｔ１とＴ２の時刻との差の絶対値が予め規定された時間内にある場合のみ正当」と判定する点に特徴がある。

【００３５】このためには、Ｓ４００１の処理を以下のようなステップＳ４１０１に変更することで実現できる。尚、ここでは、「予め規定された時間」を２０分間として説明するが、これ以外の時間であってもよい。また、固定的に規定される値ではなくＷｅｂサーバの起動時に初期設定される値であってもよい。Ｓ４１０１では、送られてきたメッセージ内の時刻とＷｅｂサーバの時刻との差分を計算し、その絶対値の大きさが２０分間以内ならば、次のステップに進む。２０分間を超えるならばＦＡＬＳＥを回答する。

【００３６】これにより、コンピュータ間に時間のズレがあった場合にも対応可能となり、かつ充分過去に生成されたメッセージは、不正であるとの判定が可能となる。しかも、時刻情報をアクセス制限にも利用できることから、一層柔軟なアクセス制限が可能となる。

【００３７】尚、ここでは、「予め規定された時間」を固定的に説明しているが、以下に示すようなユーザ名と規定時間との対応表を作成することで、ユーザ毎に可変の規定時間を適用することができる。また、下記の表における規定時間が0であった場合には、無条件にＴＲＵＥを回答するようにしてもよい。

【００３８】

規定時間（分）	ユーザ名
５０	Ａｋｉｙａｍａ
０	Ｋａｔｕｒａ
２０	Ｋｕｒｏｓａｗａ
１０	Ｓａｋａｍｏｔｏ
１２０	Ｔａｍｕｒａ
５０	Ｙａｍａｍｏｔｏ

【００３９】次に本発明の他の実施の形態としての記憶媒体について説明する。本発明をＣＰＵとメモリやＨＤ装置等でコンピュータシステムに構成する場合、上記メモリやＨＤ装置等は本発明による記憶媒体を構成する。

即ち、前述した各実施の形態で説明したフローチャートによる動作を実行するためのソフトウェアのプログラムコードを記憶した記憶媒体をシステムや装置で用い、そのシステムや装置のＣＰＵが上記記憶媒体に格納されたプログラムコードを読み出し、実行することにより、本発明の目的を達成することができる。

【００４０】また、この記憶媒体としては、ＲＯＭ、ＲＡＭ等の半導体メモリ、光ディスク、光磁気ディスク、磁気媒体等を用いてよく、これらをＣＤ－ＲＯＭ、フロッピィディスク、磁気媒体、磁気カード、不揮発性メモリカード等に構成して用いてよい。

【００４１】従って、この記憶媒体を各実施の形態で説明したシステムや装置以外の他のシステムや装置で用い、そのシステムあるいはコンピュータがこの記憶媒体に格納されたプログラムコードを読み出し、実行することによっても、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【００４２】また、コンピュータ上で稼働しているＯＳ等が処理の一部又は全部を行う場合、あるいは記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された拡張機能ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づいて、上記拡張機能ボードや拡張機能ユニットに備わるＣＰＵ等が処理の一部又は全部を行う場合にも、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【００４３】

【発明の効果】以上説明したように、本発明によれば、クライアント側の通信装置において、ネットワーク上での認証要求を目的とするパスワードのｈａｓｈ（不可逆な加工）時に時刻情報も一緒にｈａｓｈし、ｈａｓｈ結果と時刻とを含むメッセージを作成して、サーバ側の通信装置に送信するようにしたので、クライアント側のコンピュータ内の単調に増加する時刻情報を利用することにより、単方向に1回通信を行うだけで容易に認証を行うことができる。また、同じ認証情報が重複して使用されることがないので、従来のｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ型認証よりも通信コストを少なくしながら、かつ同程度の安全性を得ることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態による認証方法と従来のｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ型認証方法を説明するための構成図である。

【図2】本発明が適用されるネットワークシステムを示すブロック図である。

【図3】Ｗｅｂサーバのハードウェア構成例を示すブロック図である。

【図4】Ｗｅｂブラウザのハードウェア構成例を示すブ

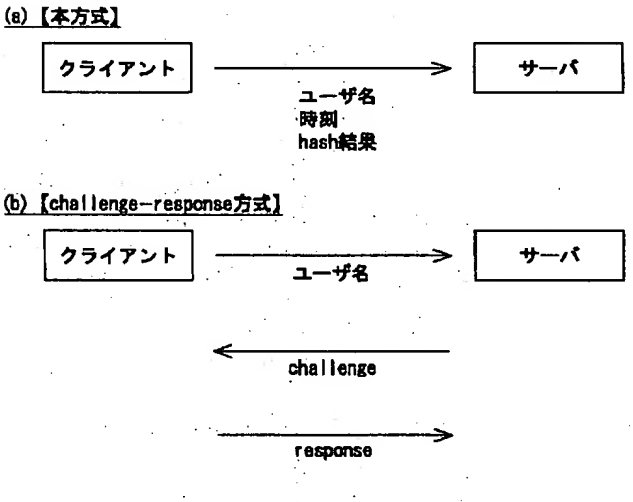
11

ロック図である。
【図5】Webサーバと Web ブラウザの構成を模式的に示すブロック図である。
【図6】Web ブラウザの処理を示すフローチャートである。
【図7】Web サーバの処理を示すフローチャートである。
【図8】hash 部の処理を示すフローチャートである。
【図9】正当性吟味部の処理を示すフローチャートである。
【符号の説明】
10、20　HD装置
11、21　メモリ
13、23　CPU
14、24　FD装置
18、28　キーボード
100　Web サーバ
101　メッセージ受信部
102　メッセージ送信部

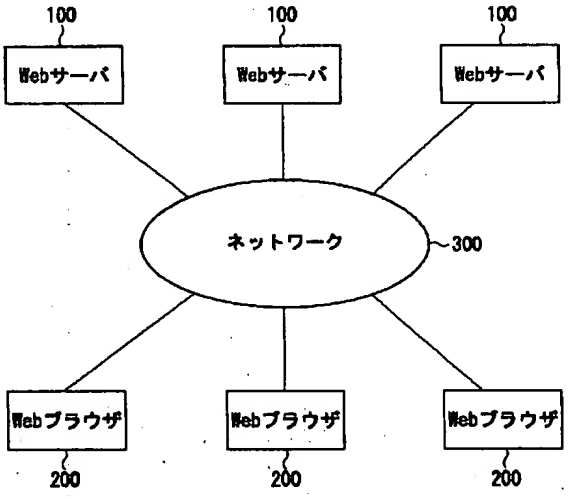
12

103　Web 情報記憶部
104　パスワード記憶部
105　時刻取得部
106　hash 部
107　正当性吟味部
200　Web ブラウザ
201　メッセージ受信部
202　メッセージ送信部
203　Web 情報指定部
204　Web 情報表示部
205　パスワード取得部
206　時刻取得部
207　hash 部
300　ネットワーク
T1　Web サーバ内の時刻
T2　送られてきたメッセージに含まれる時刻
T3　前回の正当なメッセージに含まれる時刻
H1　Web サーバ中に記憶していたパスワードから生成したhash 結果
H2　送られてきたメッセージに含まれるhash 結果

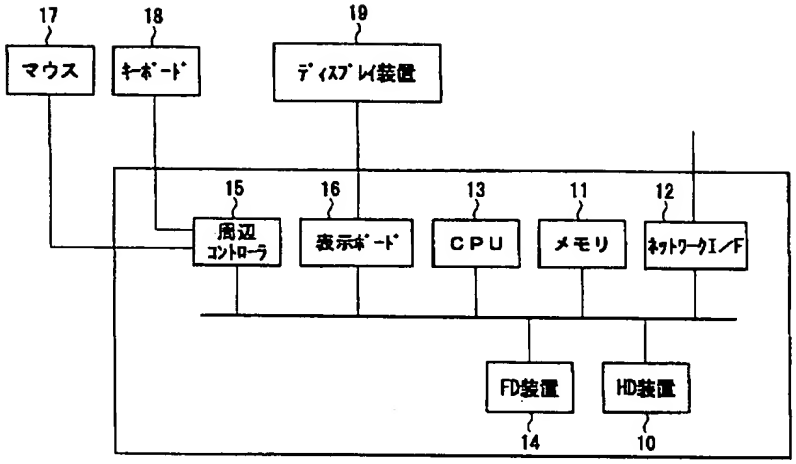
【図1】



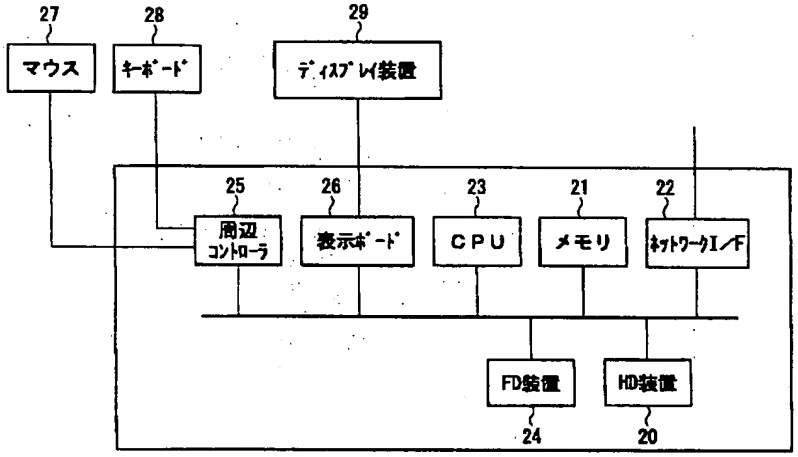
【図2】



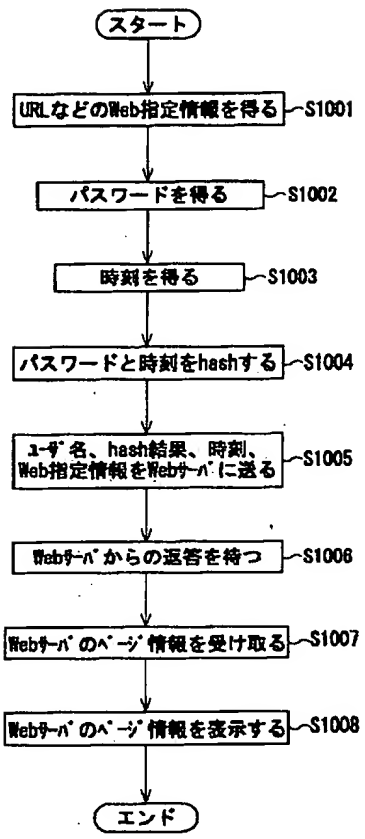
【 図3 】


17
18
19
マウス
ｷｰﾎﾞｰﾄﾞ
ﾃﾞｨｽﾌﾟﾚｲ装置
15
16
13
11
12
周辺
ｺﾝﾄﾛｰﾗ
表示ﾎﾞｰﾄﾞ
CPU
メモリ
ﾈｯﾄﾜｰｸI/F
FD装置
HD装置
14
10

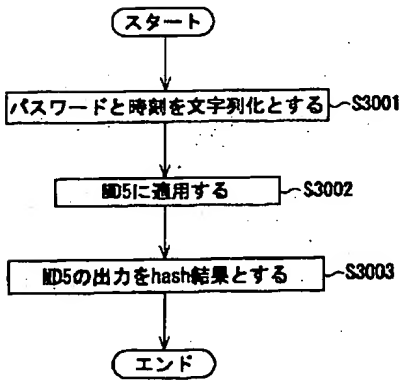
【 図4 】


27
28
29
マウス
ｷｰﾎﾞｰﾄﾞ
ﾃﾞｨｽﾌﾟﾚｲ装置
25
26
23
21
22
周辺
ｺﾝﾄﾛｰﾗ
表示ﾎﾞｰﾄﾞ
CPU
メモリ
ﾈｯﾄﾜｰｸI/F
FD装置
HD装置
24
20

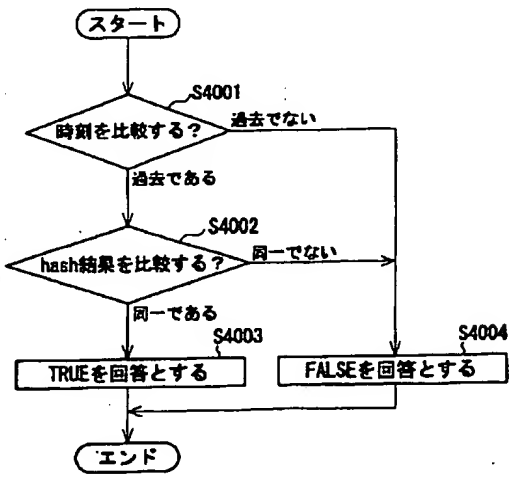
【 図6 】


スタート
URLなどのWeb指定情報を得る
S1001
パスワードを得る
S1002
時刻を得る
S1003
パスワードと時刻をhashする
S1004
ﾕｰｻﾞ名、hash結果、時刻、Web指定情報をWebｻｰﾊﾞに送る
S1005
Webｻｰﾊﾞからの返答を待つ
S1006
Webｻｰﾊﾞのﾍﾟｰｼﾞ情報を受け取る
S1007
Webｻｰﾊﾞのﾍﾟｰｼﾞ情報を表示する
S1008
エンド

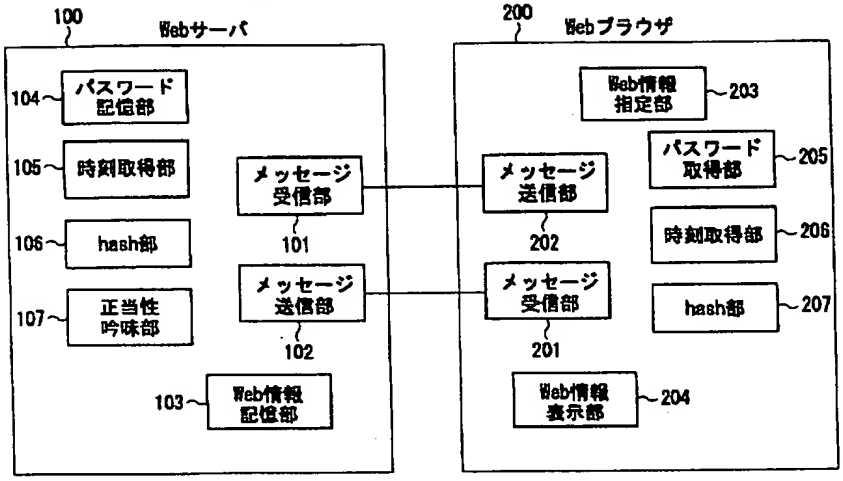
【 図8 】


スタート
パスワードと時刻を文字列化とする
S3001
MD5に適用する
S3002
MD5の出力をhash結果とする
S3003
エンド

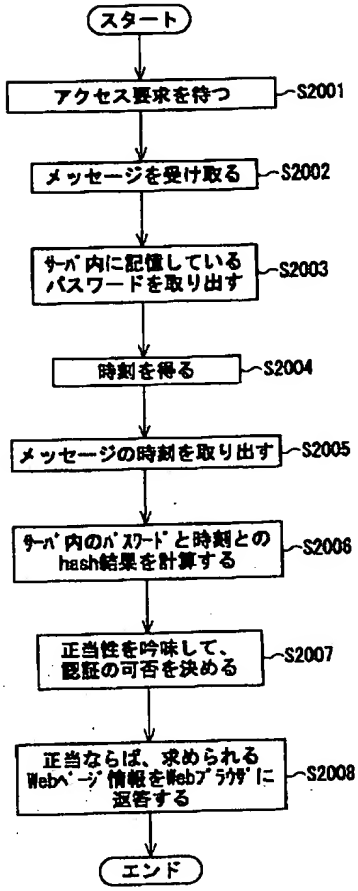
【 図9 】


スタート
S4001
時刻を比較する？
過去でない
過去である
S4002
hash結果を比較する？
同一でない
同一である
S4003
TRUEを回答とする
S4004
FALSEを回答とする
エンド

【 図5 】


100
Webサーバ
104
パスワード記憶部
105
時刻取得部
106
hash部
107
正当性吟味部
メッセージ受信部
101
メッセージ送信部
102
103
Web情報記憶部
200
Webブラウザ
Web情報指定部
203
メッセージ送信部
202
メッセージ受信部
201
パスワード取得部
205
時刻取得部
206
hash部
207
Web情報表示部
204

【 図7 】


スタート
アクセス要求を待つ
S2001
メッセージを受け取る
S2002
ｻｰﾊﾞ内に記憶しているパスワードを取り出す
S2003
時刻を得る
S2004
メッセージの時刻を取り出す
S2005
ｻｰﾊﾞ内のﾊﾟｽﾜｰﾄﾞと時刻とのhash結果を計算する
S2006
正当性を吟味して、認証の可否を決める
S2007
正当ならば、求められるWebﾍﾟｰｼﾞ情報をWebﾌﾞﾗｳｻﾞに返答する
S2008
エンド